UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
- -x

UNITED STATES OF AMERICA

- against – 19 Cr. 486 (ER)

DONALD BLAKSTAD,

Defendant.
- -x

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF MOTION TO SUPPRESS EVIDENCE SEIZED FROM DEFENDANT DON BLAKSTAD'S iCLOUD AND MICROSOFT ACCOUNTS

EUGENE IREDALE
Iredale and Yoo, APC
Counsel for DONALD BLAKSTAD
105 West F Street, 4th Floor
San Diego, California 92101
Phone: (619) 233-1525
Fax: (619) 233-3221
Email: egiredale@iredalelaw.com

I.
Facts

On 25 October 2018, the government obtained a "Search Warrant and Non-Disclosure Order" directed to Microsoft and the FBI for "all content and other information associated with the e-mail account donblakstad@msn.com." The attachment to the warrant ordered the the provider to produce all e-mails sent to or from, stored in draft form or otherwise, associated with the subject account between January 1, 2015 and October 25, 2018; "all pictures, videos, documents and files"; all web browser history for the period between January 1, 2015 and October 25, 2018; all IP logs and records of session times and duration and other related documents. The warrant then authorized "law enforcement personnel" (which included attorney support staff, agency personnel and outside technical experts) to review the records for any evidence, fruits or instrumentalities of multiple federal crimes, including categories of "evidence" related to broad categories of information vaguely connected with the investigation. (See Exhibit A, attached). There was no search protocol limiting the search to be conducted; no requirement to return, destroy or segregate information beyond the scope of the warrant; and no time period within which the search by "law enforcement personnel" was to occur.

On November 7, 2018, another magistrate judge signed a "search warrant and non-disclosure order" directed to Apple and the FBI authorizing a warrant for

"all content and other information associated with" the user ID and e-mail address donblakstad@msn.com. The attachment orders Apple to produce "all" messages from January 1, 2015, to the date of the order; "all pictures, videos, documents and files"; "all address books, contact list or similar information", "all records and other information." (See Exhibit B, attached). As with the first order, there is no search protocol required, no time period within which government personnel are to complete their search, and no requirement to segregate, destroy or return information beyond the scope of the described crimes.

For both orders, there were agent affidavits submitted. The affidavits, taken in the light most favorable to the government, set forth a recitation of probable cause that Mr. Blakstad obtained non-public information regarding Illumina's financial results to be reported in October 2016, August 2017 and October 2017, and that various other persons including Ms. Bustos, Mr. Morris and Mr. Winston participated in the events.

II.
The Warrants Were Hopelessly Overbroad On Their Face

Because the "warrants" here permitted the seizure and review of all the contents of accounts, during a period beginning a year and a half before any evidence of wrongdoing, and ending two years after any suggestion of illegality, there was temporal overbreadth. Because the warrant allowed review and retention of everything, no matter how personal, how unrelated to criminality or how

innocuous, the warrant was facially overbroad as to the scope of the search. Because the warrant imposed no reasonable limitation as to time of execution or the need to segregate, discard or return items beyond the reasonable scope of the warrant, it conferred unbounded discretion upon the government agents.

Further, it is believed that attorney-client communications with multiple attorneys were reviewed, without any attempt to reflect to attorney-client privilege.

III.
The Searches Violated The Fourth Amendment

Because this case involves mobile-phone searches, the proper constitutional context requires a brief review of the recent decision in *Riley v. California*, 134 S. Ct. 2473 (2014). There, the Supreme Court explained:

> Cell phones differ in both a quantitative and a qualitative sense from other objects . . . . One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy . . . . The storage capacity of cell phones [however] has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible.
>
> ***
>
> "Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.

> Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.
>
> "In 1926, Learned Hand observed . . . that it is 'a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is."

Id. at 2489-91 (citations omitted).

What logically follows from the Supreme Court's discussion is that, when it comes to today's mobile phones, courts must be especially vigilant to ensure the warrants authorizing their search adhere strictly to the Fourth Amendment's requirements. *See Go-Bart Importing Co. v. United States*, 282 U.S. 344, 357 (1931) ("The Amendment is to be liberally construed and all owe the duty of vigilance for its effective enforcement lest there shall be impairment of the rights for the protection of which it was adopted."). Otherwise, the government will be permitted broad access to a vast amount of our most private information, without the proper Fourth Amendment scrutiny. Here, that is precisely what occurred.

The Fourth Amendment provides, "no Warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The Fourth Amendment thus has a "requirement as one of 'specificity' and [has] distinguished its 'two

aspects': 'particularity and breadth." *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 702 (9th Cir. 2009) ("*SDI*"). "Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based.'" Both requirements "serve a common purpose: to protect privacy by prohibiting 'a general, exploratory rummaging in a persons belongings[,]'" but "they achieve the purpose in distinct ways." *United States v. Weber*, 915 F.2d 1282, 1285 (9th Cir. 1990).

For a warrant to pass muster, "[t]he two separate rules must both be met[.] *Id.* at 1286. In this case, neither was.

The particularity requirement "means that 'the warrant must make clear to the executing officer exactly what it is that he or she is authorized to search for and seize.' 'The description must be specific enough to enable the person conducting the search reasonably to identify the things authorized to be seized.'" *SDI*, 568 F.3d at 702 (citation omitted). "The particularity rule requires the magistrate to make sure that the warrant describes things with reasonable precision, since vague language can cause the officer performing the search to seize objects 'on the mistaken assumption that they fall within the magistrate's authorization.'" *Weber*, 915 F.2d at 1285.

As discussed below, there were myriad particularity problems with this list.

First, the descriptions allowed the searching agents considerable – and unconstitutional – discretion in decided what to seize and examine. Second, the descriptions were overly general, placing no meaningful restrictions on the search. This was especially problematic because more case-specific criteria were readily available to the government. Finally, the warrants failed on particularity grounds because they lacked sufficient methodology or protocols to control the manner and extent of the search.

As written, the warrants provided the agents with significant searching discretion. This directly violated the core Fourth Amendment principle that, "[a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927).

"It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment." *United States v. Bridges*, 344 F.3d 1010 at 1014 (9th Cir. 2003). Thus, a warrant must place clear limitations on what can be seized and searched.

The descriptions in the attachments, however, were impossible to satisfy without seizing and searching the phone's entire contents. For instance, only by looking at *everything* could the agents determine what information was "evidence" of the specified crimes.

Moreover, the government cannot save the searches by arguing the general descriptions were necessary. *See United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986) ("Warrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible"). On this issue, the question is whether the government could "describe the items more particularly in light of the information available to it at the time the warrant was issued[.]" *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986). Here, plainly it could have.

Rather, borrowing language from *Spilotro*, "the warrants . . . authorize[d] wholesale seizures of entire categories of items not generally evidence of criminal activity, and provide[d] no guidelines to distinguish items used lawfully from those the government had probable cause to seize." *Spilotro*, 800 F.2d at 964. The Fourth Amendment, however, required more. *See id.* The searches cannot stand.

There is an additional particularity failure that must be addressed. It is true that the government describes a place to be searched--a cellular telephone, and its stored contents. Certainly, this describes the actual thing to be searched. An electronic search, however, is not as simple.

In the context of electronic data, a request to search should be accompanied by sufficiently specific guidelines for identifying the documents sought and those

guidelines should be followed by the officers conducting the search. This is what a search protocol is. Such a protocol must explain, with particularity, the government's methodology for determining, once it is engaged in the search, how it will determine which storage areas should be searched for data within the scope of the warrant.

The government failed to include limitation language. This is an important omission because, as written, the government is requesting it be allowed to search everywhere and seize anything regardless of whether or not the data contained therein falls under the scope of its warrant.

This is a fatal flaw. As the Court explained in *Bonner*, "[t]he search protocol employed *must be reasonably directed to identify data within the scope of the warrant in order to meet the particularity requirement*. Without this requirement, the search of the electronic data becomes 'general exploratory rummaging in a person's belongings.'" *Id.* at 28 (emphasis added, citation omitted).

Accordingly, based on the myriad shortfalls in the descriptions of the items to be searched – and lack of meaningful search protocols – the Court should find that the warrants did not satisfy the Fourth Amendment's particularity requirement.

The warrants fail because they were unconstitutionally overbroad. *See Weber*, 915 F.2d at 1285. In addition to providing clear guidance to the searcher, a warrant "must [] give legal, that is, not overbroad, instructions. Under the Fourth Amendment, this means that 'there [must] be probable cause to seize the particular thing[s] named in the warrant.'" *SDI*, 568 F.3d at 702 (citation omitted). Thus, the warrant "must be no broader than the probable cause on which it is based." *Weber*, 915 F.2d at 1285. This rule "prevents the magistrate from making a mistaken authorization to search for particular objects in the first instance, no matter how well the objects are described." *Id*. at 1285-86.

Here, the warrants were overbroad in two respects. First, they permitted the agents to examine more than the probable cause justified. Second, the warrants provided no protocol for segregating data that had a nexus to the suspected crime from data that did not.

Making matters worse, the warrants contained no explicit time limitation. They did not limit the agents' ability to seize and search old data, temporally divorced from anything in the case.

The breadth of the warrant was exacerbated by their failure to provide for the segregation of non-reviewable data – i.e., data for which there was no probable cause to search.

There was no limitation on the type of files that the government could seize or search.

As the Court held in *United States v. Bridges*, 344 F.3d 1010 (9th Cir. 2003): "[s]earch warrants, including this one, are fundamentally offensive to the underlying principles of the Fourth Amendment when they are so bountiful and expansive in their language that they constitute a virtual, all-encompassing dragnet of personal papers and property to be seized at the discretion of the State." *Bridges*, 344 F.3d at 1016.

A leading case on the proper conduct of an electronic search is *United States v. Comprehensive Drug Testing, Inc*., 621 F.3d 1162 (9th Cir. 2010) (en banc). There, the *en banc* court addressed the particularities of search warrants related to electronic data. The court "recognize[d] the reality that over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records." *Id*. at 1177. As a result, there must be "greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. *The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the*

government to gain access to data which it has no probable cause to collect." *Id*. (emphasis added).

"The remedy for an overbroad search warrant is suppression of the seized evidence." *United States v. Clark*, 31 F.3d 831, 836 (9th Cir. 1994). That is the appropriate remedy here.

Although it will almost certainly try, the government cannot rely on the "good faith" exception. *United States v. Leon*, 468 U.S. 897, 926 (1984). This Court should be "vigilant in scrutinizing officers' good faith reliance on [] illegally overbroad warrants." *United States v. Kow*, 58 F.3d 423, 428 (9th Cir. 1995) (internal quotations omitted). When a warrant lists "broad classes of documents without specific description of the items to be seized," and contains no date-based restriction on those items, "the warrant [is] overbroad [such] that agents could not reasonably rely on it." *Id*. (internal quotations omitted); *see also Weber*, 915 F.2d at 1289 (the government could not rely on the good faith exception because, "at the time [the agent] applied for the warrant, the law was clear that a warrant could not be broader than the probable cause on which it was based."). That is situation here.

Moreover, suppression is especially appropriate, because it furthers the "prime purpose of the exclusionary rule[,] to deter future unlawful police conduct and thereby effectuate the guarantee of the Fourth Amendment against

unreasonable searches and seizures." *Illinois v. Krull*, 480 U.S. 340, 347 (1987) (internal quotation marks omitted).

Dated: May 29, 2020

Respectfully submitted,

/S/ *Eugene Iredale*

EUGENE IREDALE
Iredale and Yoo, APC
Counsel for DONALD BLAKSTAD
105 West F Street, 4th Floor
San Diego, California 92101
Phone: (619) 233-1525
Fax: (619) 233-3221
Email: egiredale@iredalelaw.com

CERTIFICATE OF SERVICE

I hereby certify that on May 29, 2020, I electronically filed Defendant's (1) Memorandum Of Points And Authorities In Support Of Motion To Suppress Evidence Seized From Defendant Don Blakstad's iCloud And Microsoft Accounts with the Clerk of the District Court using its CM/ECF system, which would then electronically notify the parties in this case:

Edward Arthur Imperatore, AUSA.

Respectfully submitted,

/S/ *Eugene Iredale*

EUGENE IREDALE
Iredale and Yoo, APC
Counsel for DONALD BLAKSTAD
105 West F Street, 4th Floor
San Diego, California 92101
Phone: (619) 233-1525
Fax: (619) 233-3221
Email: egiredale@iredalelaw.com